UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/701,308	11/04/2003	Kenneth J. Krieter	1300US2	5295

25279 7590 05/29/2009

GRACO MINNESOTA INC
PO BOX 1441
MINNEAPOLIS, MN 55440

EXAMINER	
AGWUMEZIE, CHARLES C	
ART UNIT	PAPER NUMBER
3685	

MAIL DATE	DELIVERY MODE
05/29/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte KENNETH J. KRIETER, MARK A. KING, CHRISTIAN D. KOCH, THOMAS C. NEESE, EUGENE G. THURY, MICHAEL J. MARSHIK, STEVEN R. KNOP, DAVID J. LORDEN, and GREGORY W. PARKHURST

Appeal 2009-3632
Application 10/701,308
Technology Center 3600

Decided: [1] May 29, 2009

Before, MURRIEL E. CRAWFORD, JOSEPH A. FISCHETTI and BIBHU R. MOHANTY, *Administrative Patent Judges*.

FISCHETTI, *Administrative Patent Judge*.

DECISION ON APPEAL

---

[1] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, begins to run from the decided date shown on this page of the decision. The time period does not run from the Mail Date (paper delivery) or Notification Date (electronic delivery).

STATEMENT OF THE CASE

Appellants seek our review under 35 U.S.C. § 134 of the Examiner's final rejection of claims 1-3. We have jurisdiction under 35 U.S.C. § 6(b)(2002).

SUMMARY OF DECISION

We AFFIRM.

THE INVENTION

Appellants claim an on-site initialization method for tank level monitoring which is said to allow for uniform mass production of system modules, preventing the need to uniquely program each module. (Spec. 3: 15-20).

Claim 1, reproduced below, is representative of the subject matter on appeal.

1. A method for registering and communicating between a central control authorization point and a plurality of remote location devices comprising the steps of:

providing a said remote location device;
preparing said remote location device for registration;
registering said remote location device on said central control authorization point and assigning and transmitting an encrypted address unique to each said remote location device from said central control authorization point and storing said unique address on said remote location device; and
utilizing said unique encrypted address for communication between said central control authorization point and said remote location device.

THE REJECTION

The Examiner relies upon the following as evidence of unpatentability:

Johnson, Jr.	6,078,888	Jun. 20, 2000
Rogers	US 2002/0049549 A1	Apr. 25, 2002

The following rejections are before us for review.

The Examiner rejected claims 1-3 under 35 U.S.C. § 103(a) over Rogers in view of Johnson.

ISSUE

Have Appellants shown that the Examiner erred in rejecting claims 1-3 on appeal as being unpatentable under 35 U.S.C. § 103(a) over Rogers in view of Johnson on the grounds that a person with ordinary skill in the art would understand that Johnson discloses registering a tag as a remote location device on a POS device 200 which POS device serving as a central point assigning and transmitting an encrypted address unique to the tag?

FINDINGS OF FACT

We find the following facts by a preponderance of the evidence:

1. The Examiner found "…Johnson discloses initial configuration of tag 100 (see col. 8, lines 55-65, which discloses that 'when initially configuring tag 100, the host network 300 generates a tag identification number...')." (Ans. 5).

2. The Examiner further found:

> … Rogers et al does not explicitly teach is transmitting an encrypted address unique to each remote location device….
>
> Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Rogers et al and incorporate a method of transmitting an encrypted address unique to each remote location device as taught by Johnson Jr. in

> order to uniquely identify each remote location device before authorization of the transaction and further ensure security. (Ans. 4).

3. Johnson discloses that

> [w]hen initially configuring tag 100, the host network 300 generates a tag identification number (ID) and a main tag key, which is preferably a DES key, and directly injects these numbers into the tag 100 along with any other pertinent information. Generally, the POS device 200 is not used during configuration. Preferably, a different main tag key is injected into every tag 100, and a secure algorithm is used to generate the main tag keys from a master key known only by the host 300. Maximum security is obtained when it is impossible for an infiltrator or cracker to calculate the host master key from the main tag key and tag ID. (Johnson, col. 8, ll. 55-65).

4. Johnson discloses that the POS system interfaces with the host system in that:

> [t]he POS device 200 preferably includes a controller 202 forming communication electronics 204 and cryptography electronics 206. The controller 202 is associated with a memory 210 and an antenna 208 for providing remote communications. The controller 202 interfaces with the telephone network 30 to provide bi-directional communications with the host network 300. Those skilled in the art will appreciate that any suitable form of communications between the POS device 200 and host network 300 are considered within the scope of this disclosure and the claims that follow…. In the preferred embodiment, the POS device 200 is a fuel dispenser having at least two fueling positions and a card reader 216 for receiving payment through any variety of

credit, debit or smartcards. (Johnson, col. 7, ll. 40-56).

5. In general, remote communication units 100 are adapted to communicate with and through the POS device 200 in order to obtain authorization and communicate information to and from the host network 300. (Johnson, col. 5, ll. 50-55).

6. Johnson discloses that before a transaction takes place, the host system first determines whether an authorized tag is being used (Johnson, col. 3, ll. 14-20).

PRINCIPLES OF LAW

"Section 103 forbids issuance of a patent when 'the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.'" *KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1734 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, (3) the level of skill in the art, and (4) where in evidence, so-called secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966). *See also KSR*, 127 S.Ct. at 1734 ("While the sequence of these questions might be reordered in any particular case, the [*Graham*] factors continue to define the inquiry that controls.")

ANALYSIS

We affirm the rejection of claims 1-3. The Appellants do not provide a

substantive argument as to the separate patentability of claims 2 and 3 that depend from claim 1 which is the sole independent claim among those claims. Therefore, regarding the claims whose rejection is affirmed, we address only claim 1. Claims 2 and 3 fall with claim 1. *See,* 37 C.F.R. § 41.37(c)(1)(vii)(2004).

Appellants argue that

> … Johnson transmits the tag identifier from the tag to the POS device (column 3, lines 10-17). Applicants' claimed invention however assigns and communicates a unique identifier from the central control authorization point into each remote device. Again, this limitation is nowhere shown nor suggested in the references of record. (Reply Br. 2-3).

The Examiner however maintains that Johnson discloses assigning and transmitting an encrypted address unique to a remote location device by finding that Johnson discloses initially configuring tag 100 by the host network 300 generating a tag identification number (FF 1).

We agree with the Examiner. Appellants' claim requires registering and communicating between a central control authorization point and a plurality of remote location devices. Thus, the claims only require that the central control authorization point be a location from where registering and communicating occur. In Johnson, this point is the POS device 200, which although called a POS device, is disclosed as not used as a POS device during configuration (FF 3), but nevertheless is the point through which the host network communicates to the tags (FF 5). Appellants argue that this assigning and transmitting of an encrypted address by the host network resembles factory configuration, rather than one affected by a central control authorization point (Reply Br. 2). However, Johnson

discloses that the host network 300 even if considered as a factory configuration device, nevertheless acts through a central authorization point e.g., the POS device 200 when it is not functioning as a POS device, to effect assigning and transmitting of an encrypted address (FF 1, 4, 5).

Appellants next argue that

> …Johnson transmits the tag identifier from the tag to the POS device (column 3, lines 10-17). Applicants' claimed invention however assigns and communicates a unique identifier from the central control authorization point into each remote device. Again, this limitation is nowhere shown nor suggested in the references of record. (Reply Br. 2-3).

We disagree with Appellants. A closer reading of this excerpt in Johnson reveals that the referenced communication between the tag and the POS device occurs only for transactions, and is based on the host system first determining whether an authorized tag is being used (FF 6), and not as part of the configuration process. Accordingly, Appellants' argument is not persuasive as to error in the rejection.

Appellants further argue that "[t]here is no suggestion or motivation as to how or why one would apply Johnson Jr. to Rogers …." (Reply Br. 3). We disagree with Appellants. To the extent Appellants seek an explicit suggestion or motivation in the reference itself, this is no longer the law in view of the Supreme Court's recent holding in *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1741 (2007). Since the Examiner has provided some articulated reasoning with some rational underpinning for why a person with ordinary skill in the art would modify

Guthrie to use wireless communication for inventorying, e.g., transmitting an encrypted address unique to each remote location device in order to uniquely identify each remote location device before authorization of the transaction and further ensure security (FF 2), Appellants' argument is not persuasive as to error in the rejection.

Thus, for the above reasons we sustain the rejection of claims 1-3.

CONCLUSION OF LAW

We conclude the Appellants have not shown that the Examiner erred in rejecting claims 1-3 under 35 U.S.C. § 103(a) as unpatentable over Rogers in view of Johnson.

DECISION

The decision of the Examiner to reject claims 1-3 is AFFIRMED.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 1.136(a)(1)(iv) (2006).

AFFIRMED

JRG

GRACO MINNESOTA, INC.
P.O. BOX 1441
MINNEAPOLIS, MN 55440